PA000310

SECURE GENERATION OF TEMPORARY MOBILE STATION IDENTIFIERS

BACKGROUND

FIELD

[1001] The present invention generally relates to wireless communication systems and more particularly to secure generation of temporary mobile station identifiers.

RELATED ART

[1002] In wireless communication systems, such as Global System for Mobile Communication ("GSM"), each mobile station uses an International Mobile Subscriber Identifier ("IMSI") to uniquely identify each user on the network. However, an attacker or eavesdropper may use a mobile station's IMSI to potentially track or eavesdrop on a mobile station user. In order to obscure the identity of the mobile user some systems, such as GSM and the Code Division Multiple Access ("CDMA") Interim Standard 2000 ("IS-2000"), use Temporary Mobile Station Identifier ("TMSI") in lieu of IMSI when operating in a service area.

[1003] TMSI provides security by substituting a randomly selected identification number instead of the mobile station's actual IMSI. The TMSI is selected from a large pool of possible identifiers. In GSM and CDMA IS-2000 systems the TMSI value is a thirty two (32) bit number. Thus, for GSM and CDMA the number of possible TMSI that can be assigned is 2^{32} or 4,294,967,296.

[1004] This number provides a large number of possible TMSI assignments. The security of TMSI is derived from its large space of possible assignments that an eavesdropper must search to find a particular user. However, the total number of assignments is currently too large for current systems to manage as an assignment table in real time. Also, managing such a large table in memory requires a large amount of memory, which adds to manufacturing costs.

[1005] Some known methods for managing and assigning TMSI are as follows. One method is to select TMSIs randomly. However, a problem with a random selection is that it is possible that two or more mobile stations have the same randomly-assigned TMSI. If the network assigns about 2^{16} TMSI, the probability that an identical assignment was made approaches one.

[1006] A second method is to assign TMSIs from a small subset of the total space to speed searches. Although this approach reduces the storage requirements, it also reduces the randomness of the TMSI. This weakens the overall strength of the TMSI protection scheme, since an eavesdropper has a better chance of predicting the next TMSI assignment, based on the current assignment.

[1007] A third method is to manage TMSI assignments as a linked list. Using a linked list minimizes the storage required. However, a linked list approach greatly increases the search time to find an entry for a TMSI or to find an unassigned TMSI for a new assignment.

[1008] Thus, it is beneficial for a wireless system to be able to practically maintain and generate secure temporary mobile station identifiers. There is

therefore a need in the art for methods and systems for efficiently maintaining and securely generating TMSI assignments.

SUMMARY

[1009] Embodiments disclosed herein address the above stated needs by using an encryption module to securely generate a TMSI and storing the corresponding IMSI in an assignment table, which holds N entries, where N is determined based on the maximum number of expected users U, supported by a service area.

[1010] The presently disclosed embodiments are directed to methods and systems for efficiently maintaining and securely generating TMSI assignments. According to one aspect of the present invention, a visitor location register first initializes an assignment table to store N entries. Next, the visitor location register waits until a TMSI assignment is needed. Then, a counter is maintained in memory and is incremented. The value of the counter is then hashed to produce an assignment table index. Beginning at the assignment table index, the assignment table is searched for an available entry. The counter is then encrypted to produce a TMSI. The IMSI corresponding to the TMSI assignment is then stored in the assignment table.

BRIEF DESCRIPTION OF THE DRAWINGS

[1011] FIG. 1 illustrates an exemplary service area in a wireless communication system according to an embodiment of the present invention.

[1012] FIG. 2 illustrates an exemplary procedure for generating and maintaining temporary mobile station identifiers according to an embodiment of the present invention.

[1013] FIG. 3 illustrates an exemplary alternative procedure for generating and maintaining temporary mobile station identifiers according to an embodiment of the present invention.

DETAILED DESCRIPTION

[1014] The presently disclosed embodiments are directed to methods and systems for efficiently maintaining and securely generating TMSI assignments. The following description contains specific information pertaining to the implementation of the present invention. One skilled in the art will recognize that the present invention may be implemented in a manner different from that specifically discussed in the present application. Moreover, some of the specific details of the invention are not discussed in order not to obscure the invention. The specific details not described in the present application are within the knowledge of a person of ordinary skill in the art.

[1015] The drawings in the present application and their accompanying detailed description are directed to merely example embodiments of the invention. To maintain brevity, other embodiments of the invention which use the principles of the present invention are not specifically described in the present application and are not specifically illustrated by the present drawings. The word "exemplary" is used exclusively herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not

necessarily to be construed as preferred or advantageous over other embodiments.

[1016] FIG. 1 illustrates exemplary service area 100 operating in a wireless communications system, wherein service area 100 uses a temporary identifier, such as TMSI, to provide user identity confidentiality. Service area 100 may be any system using temporary identifiers, such as a GSM communication system or a CDMA communication system.

[1017] By way of example, the present embodiment of the invention operates in a CDMA communication system. The general principles of CDMA communication systems, and in particular the general principles for generation of spread spectrum signals for transmission over a communication channel is described in U.S. patent 4,901,307 entitled "Spread Spectrum Multiple Access Communication System Using Satellite or Terrestrial Repeaters" and assigned to the assignee of the present invention. The disclosure in that patent, i.e. U.S. patent 4,901,307, is hereby fully incorporated by reference into the present application. Moreover, U.S. patent 5,103,459 entitled "System and Method for Generating Signal Waveforms in a CDMA Cellular Telephone System" and assigned to the assignee of the present invention, discloses principles related to PN spreading, Walsh covering, and techniques to generate CDMA spread spectrum communication signals. The disclosure in that patent, i.e. U.S. patent 5,103,459, is also hereby fully incorporated by reference into the present application. Further, the present invention utilizes time multiplexing of data and various principles related to "high data rate" communication systems, and the

present invention can be used in a "high data rate" communication systems, disclosed in U.S. patent application entitled "Method and Apparatus for High Rate Packet Data Transmission" Serial No. 08/963,386 filed on November 3, 1997, and assigned to the assignee of the present invention. The disclosure in that patent application is also hereby fully incorporated by reference into the present application.

[1018] Service area 100, generally may contain many users, each operating a mobile station, such as mobile station 112. Mobile station 112, for example, may be a cellular phone or a wireless modem. Mobile station 112 transmits a radio frequency ("RF") signal by way of antenna 114 to a base station, such as base station 126 or 136. Base station 126 receives the RF signal transmitted from mobile station 112 by way of antenna 124. Similarly, base station 136 receives the RF signal transmitted from mobile station 112 by way of antenna 124. Base station 126 and base station 136 are controlled by base station controller 128. Base station controller 128 operates with mobile switching center 130, which acts as a switching node for service area 100. Also, mobile switching center 130 provides the functionality for setting up a call, such as registration, authentication, location update, and call routing for mobile station 112.

[1019] Mobile switching center 130 coordinates with visitor location register ("VLR") 132 and home location register ("HLR") to provide call-routing and roaming capabilities for mobile station 112; the HLR is not shown in FIG. 1. As part of call-routing and roaming, VLR 132 provides a TMSI assignment for mobile station 112 as it begins operating in service area 100. When a TMSI assignment

is granted for mobile station 112, VLR 132 maintains an entry in assignment table 140 that stores the IMSI value of mobile station 112. In maintaining assignment table 140, VLR 132 also uses counter 142 and encryption module 144, which are discussed in further detail in FIG. 2.

[1020] FIG. 2 illustrates procedure 200, which is used for the generation and management of temporary identifiers, such as TMSI for mobile stations. In general, procedure 200 resides in a visitor location register, such as VLR 132. Procedure 200 begins in step 202. In step 204, VLR 132 initializes assignment table 140 to hold N entries, wherein service area 100 supports U users. The number of entries N is chosen such that $N > U$, because the system efficiency degrades significantly as the number of utilized entries approaches the size of the hash table, i.e. as U approaches N. An exemplary general rule, corresponding to a particular efficiency level, states that the hash table should be approximately two-thirds full, i.e. $N \geq 1.5U$. See, for example, "The Art of Computer Programming," Vol. 3, by Donald E. Knuth, published in 1998 by Addison-Wesley Publishing Company, with ISBN number 0-201-89685-0. Assignment table 140 stores a subscriber identifier, such as an IMSI, for each assigned TMSI. VLR 132 uses assignment table 140 to obtain the corresponding IMSI for a TMSI assigned to mobile station 112.

[1021] In step 206, VLR 132 waits until a TMSI assignment is needed, such as when mobile station 112 enters a new serving system, wherein each serving sector comprises a VLR.

[1022] In step 208, VLR 132 increments counter 142, which is a K-bit counter, where K bits is the same length as the identifier used by the TMSI. Counter 142 is initialized to zero at the time of installation. Before each new TMSI assignment, counter 142 is incremented. In GSM and CDMA, the TMSI is a thirty two (32) bit number, thus counter 142 is configured to be a thirty two (32) bit counter.

[1023] In step 210, counter 142 is hashed to obtain an assignment table index. A hash function module generates an assignment table index that ranges from 0 to N-1. A standard hash function can be used, such as those found in "The Art of Computer Programming," Vol. 3, by Donald E. Knuth, published in 1998 by Addison-Wesley Publishing Company, with ISBN number 0-201-89685-0. The hash function module output determines the starting index in assignment table 140, assignment table index.

[1024] In step 212, VLR 132 begins searching for an available entry beginning with the entry at "assignment table index." If the entry located at assignment table index has a TMSI assigned to it, then VLR 132 repeats the search at the next entry. For example, if the assignment table index is X, and entry X in the assignment table index has a TMSI assigned to it, then VLR 132 resumes its search at entry X+1 in the assignment table. The search is repeated until an entry that does not have a TMSI assignment is found. To prevent problems when the end of a table is reached, for example, the program should also have a provision such that if $X+1 \geq N$, the search would resume at index = 0 in the table.

[1025] In step 214, VLR 132 encrypts the value of counter 142, which will be referred to as "counter value" in the present application. The TMSI is generated in step 214 by encryption of the counter value. VLR 132 uses an encryption algorithm with a K-bit block cipher, where again, K is the same length as the identifier used by the TMSI. For example, a CDMA or GSM system would use an encryption algorithm with a 32-bit block cipher. An encryption algorithm provides a one-to-one mapping between the counter value and a corresponding TMSI assignment. Thus, collisions from assigning the same TMSI value are avoided provided that the same counter value is not used concurrently by different TMSI assignments. To provide further security, the ciphering key is known only to VLR 132 to hinder an attacker from correctly identifying the next TMSI that is assigned.

[1026] In step 216, after VLR 132 generates a TMSI assignment, VLR 132 stores the IMSI of mobile station 112 and counter value in assignment table 140. After step 216, the procedure continues at step 206 for the next TMSI assignment.

[1027] After assignment table 140 is populated with one or more entries using procedure 200, VLR 132 may obtain the corresponding IMSI of an assigned TMSI. When VLR 132 receives a TMSI from mobile station 112, VLR 132 obtains the IMSI of mobile station 112 by first decrypting the TMSI. The decrypted TMSI reveals the counter value of the 32-bit counter. The counter value is then passed to a hash function as in step 210, which produces the assignment table index value corresponding to mobile station 112. Starting from

the entry corresponding to the index value, assignment table 140 is searched until a match is found with the counter value. The entry corresponding to the counter value contains the correct IMSI value of mobile station 112.

[1028] Generally, VLR 132 stores an additional table, which may be referred to as an IMSI-to-TMSI table, in which the TMSI is stored for each active IMSI. This table can be used, for example, if the network is trying to page a mobile station. First, the network presents IMSI corresponding to mobile station 112, for example. Then, VLR 132 uses the IMSI-to-TMSI table to obtain the TMSI corresponding to mobile station 112.

[1029] Also, the IMSI-to-TMSI table allows an assigned TMSI to be removed if an IMSI registration is cancelled or expired. For example, VLR 132 may receive an order from the network to remove an IMSI registration. Thus, the corresponding TMSI entry must be removed from assignment table 140.

[1030] VLR 132 obtains the corresponding TMSI value associated with the IMSI from the IMSI-to-TMSI table. The TMSI is decrypted, which then produces a counter value. The counter value is hashed to reveal an assignment table index. The table is then searched starting from the entry corresponding to the assignment table index. The entry corresponding to the counter value is then removed, thus freeing that TMSI for future use.

[1031] Generally, VLR 132 can use a timer to ensure that a TMSI value expires after a certain time. This timer should be sufficiently short so that counter 142, which is thirty two bits in one embodiment, does not wrap around to a value that corresponds to an active TMSI assignment.

[1032] FIG. 3 illustrates procedure 300, which is an alternative approach for the generation and management of temporary identifiers, such as TMSI for mobile stations. Procedure 300 is particularly useful in cases where the number of entries N is a power of two, wherein service area 100 supports U users. Procedure 300 works for any N value, although the division and modulus operations are particularly efficient for values that are powers of two. In general, procedure 300 resides in a visitor location register, such as VLR 132.

[1033] Procedure 300 begins in step 302. In step 304, VLR 132 initializes assignment table 140 to hold N entries. As shown in step 304, N may be chosen such that it is a power of two, however this is exemplary. Assignment table 140 stores an IMSI value for each assigned TMSI value. VLR 132 uses assignment table 140 to obtain the corresponding IMSI value for a TMSI assigned to mobile station 112.

[1034] In step 306, VLR 132 waits until a TMSI assignment is needed, such as when mobile station 112 enters a new serving system. In step 308, counter 142 is a K-bit counter, where K bits is the same length as the identifier used by the TMSI. Counter 142 is initialized to zero at the time of installation. Before each new TMSI assignment, counter 142 is incremented. In GSM and CDMA, the TMSI is a thirty two bit number, thus counter 142 is configured to be a thirty two (32) bit counter.

[1035] In step 310, counter 142 is hashed to obtain an assignment table index. The hash function generates an assignment table index that ranges from 0 to N -1. A standard hash function similar to the one described in step 210 can

be used. The hash function output determines the starting index in assignment table 140, assignment table index.

[1036] In step 312, VLR 132 begins searching for an available entry beginning with the entry at assignment table index. If the entry located at the assignment table index has a TMSI assigned to it, then VLR 132 repeats the search at the next entry. For example, if the assignment table index is X, and entry X in the assignment table index has a TMSI assigned to it, then VLR 132 repeats the search at entry X+1 in the assignment table. The search is repeated until an entry that does not have a TMSI assignment is found. As mentioned in the discussion of step 212, the program should also have a provision such that if X+1 $\geq$ N, the search would resume at index = 0 in the table.

[1037] In step 314, VLR 132 encrypts the following to generate a TMSI assignment:

$$N \times (\text{Count}/N) + \text{Index},$$

where Count is the counter value and Index is the assignment table index generated in step 312, and the multiplication and division operations use standard integer arithmetic. In this case, the decrypted TMSI directly reveals the table index at which the IMSI is stored.

[1038] As with procedure 200, VLR 132 uses an encryption algorithm with a K-bit block cipher, where K is the same length of the identifier used by the TMSI. Also, to provide further security, the ciphering key is known only to VLR 132 to hinder an attacker from correctly identifying the next TMSI that is assigned.

[1039] In step 316, after VLR 132 generates a TMSI assignment, VLR 132 stores the IMSI of mobile station 112 in assignment table 140. After step 316, the procedure proceeds to step 306 for the next TMSI assignment.

[1040] After assignment table 140 is populated with one or more entries using procedure 300, a VLR 132 may obtain the corresponding IMSI of an assigned TMSI, using a similar procedure to one described for procedure 200. When VLR 132 receives a TMSI from mobile station 112, VLR 132 obtains the IMSI of mobile station 112 by first decrypting the TMSI. The decrypted TMSI, modulo N, directly reveals the assignment table index corresponding to mobile station 112. Since entries are not necessarily deleted in the order they are inserted or with a particular spacing between them, a small proportion of the TMSIs may repeat after some number of additional assignments. This, however, is expected in any pseudo-random method of assigning TMSI values and does not affect system security provided that the hash function and the encryption function are well chosen. It is noted that various methods for table management, including methods for entry insertion and deletion are known in the art and can be found, for example, in "The Art of Computer Programming," Vol. 3, by Donald E. Knuth, published in 1998 by Addison-Wesley Publishing Company, with ISBN number 0-201-89685-0.

[1041] VLR 132 obtains the corresponding IMSI value of mobile station 112 by referencing the assignment table entry specified by the table index. Generally, VLR 132 stores an additional table, an IMSI-to-TMSI table, in which the TMSI is stored for each active IMSI so that the TMSI can be found for paging.

VLR 132 obtains the corresponding TMSI value associated with the IMSI from the IMSI-to-TMSI table. First, VLR 132 decrypts the TMSI of mobile station 112. The decrypted TMSI produces the assignment table index corresponding to mobile station 112. The entry corresponding to mobile station 112 is then removed, thus freeing that TMSI for future use.

[1042] Generally, VLR 132 can use a timer to ensure that TMSI values expire after a certain time. This timer should be sufficiently short so that counter 142, which is thirty two (32) bits in one embodiment, does not wrap around to a value that corresponds to an active TMSI assignment.

[1043] Thus, in the manner described above, the invention provides methods and systems for efficiently maintaining and securely generating TMSI assignments. Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[1044] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in

terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[1045] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor ("DSP"), an application specific integrated circuit ("ASIC"), a field programmable gate array ("FPGA") or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[1046] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. The software module, also called a computer program in the present application, may contain a number of source code or object code segments and may reside in any

computer readable medium such as a RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, a DVD-ROM or any other form of computer readable medium known in the art. An exemplary computer readable medium is coupled to the processor, where the processor can read information from, and write information to, the computer readable medium. In the alternative, the computer readable medium may be integral to the processor. The processor and the computer readable medium may reside in an ASIC. The ASIC may reside in a mobile unit, base station transceiver, or satellite transponder. In the alternative, the processor and the computer readable medium may reside as discrete components in a user terminal.

[1047] The above description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.